NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.81

3/19/99

Cancellation Date: 3/19/00

SUBJ: GUIDELINES FOR THE SOFTWARE REVIEW PROCESS

1. PURPOSE. This notice provides guidelines to Aircraft Certification Service (AIR) field offices (i.e., Aircraft Certification Offices and Manufacturing Inspection District or Satellite Offices) and to Designated Engineering Representatives (DER) regarding the application of RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," for conducting software reviews. Advisory Circular (AC) 20-115B, "RTCA, Inc. Document RTCA/DO-178B," recognizes DO-178B as an acceptable means of compliance for securing the Federal Aviation Administration's (FAA) approval of software in airborne systems and equipment. This notice establishes guidelines for conducting software reviews during the software development life cycle of airborne systems and equipment that are developed to meet the objectives of DO-178B.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all Aircraft Certification Offices (ACO), all Manufacturing Inspection Offices (MIO), all Manufacturing Inspection District or Satellite Offices (MIDO/MISO), and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the FAA Academy.

3. RELATED PUBLICATIONS.

a. Advisory Circular 20-115B, "RTCA, Inc. Document RTCA/DO-178B," dated January 11, 1993.

b. RTCA, Incorporated, document RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

c. FAA Job Aid, "Conducting Software Reviews Prior to Certification," dated June, 1998.

Distribution: A-W(IR)-3; A-X(CD)-4; A-FAC-0 (ALL), A-FFS-7 (ALL); A-FFS-2,8 (LTD); AMA-220 (25 copies); AFS-600 (3 copies)

Initiated By: AIR-130

4. DEFINITIONS. For the purpose of this notice, the following definitions apply:

a. Review is the act of inspecting or examining software life cycle data, software project progress and records, and other evidence made with the intent of finding compliance with DO-178B objectives. Review is an encompassing term and may consist of a combination of reading, interviewing project personnel, witnessing activities, sampling data, and participating in presentations. A review may be conducted at one's own desk, at an applicant's facility, or at an applicant's supplier's facility.

b. Sampling is the process of selecting a representative set of software life cycle data for inspection or analysis to attempt to determine the compliance of all the software life cycle data developed up to that point in time in the project. Sampling is the primary means of assessing the compliance of the software processes and data. Examples of sampling may include any or all of the following:

(1) An inspection of the traceability from system requirements to software requirements to software design to source code to object code to test cases and procedures to test results.

(2) A review of any analyses used to determine system safety classification and software level, or of any reviews or analyses used to meet any DO-178B objective (e.g., timing analysis or code review).

(3) An examination of the structural coverage of multiple samples of source code modules.

(4) An examination of multiple samples of software quality assurance records and configuration management records.

c. Presentation is useful for providing emphasis on important issues or solutions or for clarifying points of question before the largest possible audience at the same time. Presentations should be used sparingly in assessing software, as the presentation data is general in nature and tends to provide an idealized and static abstraction of the actual processes. In obtaining review results of software life cycle processes, the productivity of presentations is typically low. Presentations combined with sampling is more effective. Presentations generally provide an overview of what was supposed to transpire during the development activities. Sampling provides a view of what actually transpired. Inconsistencies between presentation information and sampling data can provide certification authorities and designees insight into the actual life cycle activities. Inconsistencies can also provide management with important feedback data for continuous improvement.

d. Finding is the identification of a failure to show compliance to one or more of the DO-178B objectives.

e. Observation is the identification of a potential software life cycle process improvement.

5. SCOPE.

a. Section 9 of DO-178B describes the certification liaison process. The certification liaison process is the vehicle to establish communication and understanding between the applicant and the certification authority. Sections 9.2 and 10.3 of DO-178B state that the certification authority may review the software life cycle processes and data to assess compliance to DO-178B. This notice does not change the intent of DO-178B with regard to the software review process but clarifies the application of DO-178B.

b. Although desk reviews may be used to successfully accomplish the software review process, this notice primarily focuses on on-site reviews. The desk review uses similar techniques as the on-site review but does not have the advantages of being on-site (e.g., access to software personnel, access to all automation, access to test set-up). Both on-site and desk reviews may be delegated to properly authorized designees. Practical arrangements with the software developer for FAA on-site reviews should include:

(1) Agreement on the type of review(s) that will be conducted (i.e., planning, development, verification, or final certification).

(2) Agreement on date(s) and location(s) of the review(s).

(3) Identification of the certification authority's personnel involved.

(4) Identification of any designees involved.

(5) Development of the agenda(s) and expectations.

(6) Listing of software data to be made available (both prior to the review(s) and at the review(s)).

(7) Clarification of procedures intended to be used.

(8) Identification of any required resources.

(9) Specification of date(s) and means for communicating review results (may include corrective actions and other required post-review activities).

c. The objectives of the software review process are found in Section 6 of this notice. Section 7 of this notice primarily addresses the integration of the software review process with the software development life cycle. Section 7 also identifies the four types of reviews and the software life cycle data and data assessment criteria for each type. Section 8 of this notice addresses additional considerations for the software review process. Section 9 of this notice provides guidelines for preparing, conducting, and documenting the software review.

6. OBJECTIVES OF THE SOFTWARE REVIEW PROCESS.

a. The certification authority may review the software life cycle processes and associated data at his or her own discretion to obtain assurance that a software product submitted as part of a certification application complies with the certification basis and the objectives of DO-178B. The software review process assists both the certification authority and the applicant in determining if a particular project will meet the certification basis and DO-178B objectives by providing:

(1) Timely technical interpretation of certification basis and DO-178B objectives, FAA policy, issue papers, and other applicable certification requirements.

(2) Visibility into the implementation compliance and the applicable data.

(3) Objective evidence that the software project adheres to its approved software plans and procedures.

(4) The opportunity for the certification authority to monitor designee activities.

b. The amount of FAA involvement in a software project should be determined and documented as soon as possible in the project life cycle. The type and number of software reviews will depend on the software level of the project, the amount and quality of designee support, the experience and history of the applicant and/or software developer, service difficulty history, and several other factors. The specifics for determining and documenting the level of FAA involvement in software projects will be addressed in future FAA policy.

7. INTERACTION BETWEEN THE SOFTWARE REVIEW PROCESS AND SOFTWARE LIFE CYCLE.

a. The review process should begin early in the software life cycle. The early involvement will mitigate the risk that the system, software, and planning decisions will not comply with the DO-178B objectives. This requires timely communication between the applicant and ACO engineer regarding those planning decisions that may impact the software product and processes. Typically, the development of software associated with an aircraft or engine component or a Technical Standard Order (TSO) appliance may take several months or years. Since DO-178B is process-orientated guidance, to be meaningful the review process should be integrated throughout the software life cycle. This means that regular contact between the applicant and FAA should be established. This contact should provide gradually increasing confidence in the software life cycle processes and the resultant product to both the applicant and the FAA. The four types of reviews are described as follows:

(1) A software planning review should be conducted when the initial software planning process is complete (i.e., when most of the plans and standards are completed and reviewed).

(2) A software development review should be conducted when most of the software development data (i.e., requirements, design, and code) are complete and reviewed.

(3) A software verification review should be conducted when most of the software verification and testing data are complete and reviewed.

(4) A final certification software review should be conducted after the final software build is completed, the software verification is completed, a (preliminary) software conformity review has been conducted, and the software product is ready for formal system certification approval.

b. Availability of software life cycle data does not imply that the data is always complete. However, the data should be sufficiently mature so that a reasonable review can be conducted. Similarly, all transition criteria may not necessarily be complete for that time in the project, but sufficient transition criteria evidence should exist to ensure they are being applied to the project.

c. Discussions between the applicant and the FAA occurs early in the project life cycle and should determine the types, need, number, depth, and format of the software reviews. For the purpose of this notice, four reviews are identified to assess compliance to DO-178B objectives. As previously stated, the level of FAA involvement in the software project will be further documented in future policy.

d. The following paragraphs define the basic goals of each of the four types of software reviews, the criteria for each type of review (e.g., type and availability of data, type of transition criteria), and the appropriate evaluation criteria. Section 8 of this notice identifies additional considerations that may impact the type and timing of reviews.

(1) Software Planning Review

(a) Identification of the Software Planning Review. The software planning process is the initial process in the software life cycle for any software project. The planning process establishes the various software plans, standards, procedures, activities, methods, and tools required to develop, verify, control, assure, and produce the software life cycle data. The intent of the software planning review is to determine if the applicant's plans and standards provide an acceptable means for complying with the objectives of DO-l78B. This review can also reduce the risk of an applicant producing a software product inconsistent with the certification criteria and which will not support the continued airworthiness requirements of the product. The software planning review should take place after the initial completion of the software planning process. Although the software planning process may continue throughout the software life cycle, and plans and standards may change as the project progresses, it is generally considered complete when the associated initial transition criteria are satisfied. The following transition criteria are indicative of typical software planning process completion criteria:

1. Software plans and standards have been internally reviewed based on company specified criteria and deficiencies resolved.

2. Software plans and standards have been evaluated by software quality assurance and deficiencies resolved.

3. Software plans and standards have been approved and placed under configuration control.

4. The objectives of DO-178B, Annex A, Table A-1 have been satisfied.

(b) Data Required for the Software Planning Review. The applicant should make the software plans and standards shown in Table 1 available to the certification authority or designee (if appropriate). The supporting software data should be under configuration control, appropriate for the software level, prior to the software planning review.

Software Data	**DO-178B Section**
Plan for Software Aspects of Certification	11.1
Software Development Plan	11.2
Software Verification Plan	11.3
Software Configuration Management Plan	11.4
Software Quality Assurance Plan	11.5
*Software Requirements, Design, and Code Standards	11.6, 11.7, 11.8
Tool Qualification Plans, if applicable	12.2, 12.2.3.1
Software Quality Assurance Records as applied to the planning activities	4.6, 11.19

* Not required for Level D, per DO-178B, Annex A, Table A-1.

Table 1. Data Availability for Software Planning Review

(c) Evaluation Criteria for the Software Planning Review. The objectives which apply to planning in DO-178B Annex A, Tables A-1 (all objectives), A-8 (objectives 1-4), A-9 (objective 1), and A-10 (objectives 1-2), should be used as the evaluation criteria for the software planning review. Additionally, the applicant's safety assessment, failure conditions, and software level(s) should be assessed. The relevance of the software plans and standards to the software level should also be evaluated.

(2) Software Development Review

(a) Identification of the Software Development Review. The software development processes are the software requirements, design, code, and integration processes. The development processes are supported by the integral processes of software verification, configuration management, quality assurance, and certification liaison processes. Therefore, the software development review should assess the effective implementation of the applicant's plans and standards through examination of the software life cycle data, particularly the software

development data and integral processes' data associated with it. During this review, the applicant and FAA may come to agreement on changes to or deviations from plans and standards that are discovered during the review. Before conducting a software development review, the software development data should be sufficiently complete and mature to ensure that enough evidence exists that the developer is complying with their approved plans, standards, and transition criteria. The following are typical criteria for a sufficiently mature software development process:

1. High-level requirements are documented, reviewed, and traceable to system requirements.

2. Software architecture is defined, and reviews and analyses have been completed.

3. Low-level requirements are documented, reviewed, and traceable to high-level requirements.

4. Source code implements and is traceable to the low-level requirements and has been reviewed.

(b) Data Required for the Software Development Review. For a software development review, the software data shown in Table 2 should be made available to the certification authority. The supporting software data should be under configuration control, as appropriate for the software level, prior to the review.

Software Data	**DO-178B Section**
*Software Requirements, Design and Code Standards	11.6, 11.7, 11.8
Software Requirements Data	11.9
Design Description	11.10
Source Code	11.11
Software Verification Results (as applied to DO-178B, Annex A, Tables A-2 through A-5)	6.3.1, 6.3.2, 6.3.3, 6.3.4, 11.14
Software Life Cycle Environment Configuration Index	11.15
Problem Reports	11.17
Software Configuration Management Records	11.18
Software Quality Assurance Records (as applied to DO-178B, Annex A, Tables A-2 through A-6)	11.19

* Not required for Level D, per DO-178B, Annex A, Table A-1.

Table 2. Data Availability for the Software Development Review

(c) Evaluation Criteria for the Software Development Review. The objectives which apply to development in DO-178B, Annex A, Tables A-2 (objectives 1-6), A-3 (all objectives), A-4 (all objectives), A-5 (objectives 1-6), A-8 (objectives 1-4, 6), A-9 (objectives 1-2), and A-10 (objective 3), should be used as evaluation criteria for this review. Additionally, the software life cycle data should be evaluated to determine the effectiveness of the applicant's plans and standards implementation in the development process.

(3) Software Verification Review

(a) Identification of Software Verification Review. The software verification process is typically a combination of inspections, demonstrations, reviews, analyses, tests, and test coverage analysis. As with the other reviews, the software configuration management and quality assurance processes are also active during these verification activities. The verification activities confirm that the software product specified is the software product built. Therefore, the software verification review should ensure that the software verification processes will provide this confirmation and will result in objective evidence that the product has been sufficiently tested and is the intended product. The purpose of the software verification review is to: assess the effectivity and implementation of the applicant's verification plans and procedures; ensure the completion of all associated software configuration management and quality assurance tasks; ensure that the software requirements and design have been verified; and ensure that the software verification process will achieve the structural coverage criteria of DO-178B, Annex A, Table A-7. Before conducting a software verification review, the software verification process should be sufficiently complete and mature to ensure that the representative verification data exists to assess that the applicant's approved plans and standards are being complied with and evidence exists that transition criteria have been met. The following criteria are indicative of a mature verification process:

1. All development data (e.g., requirements, design, source code, object code, linking and loading data, executable image) is complete, has been reviewed, and is under configuration control.

2. Test cases and procedures are documented, reviewed, and placed under configuration control.

3. Any completed testing (either formal or informal) indicates a relatively mature product.

4. Any completed testing results are documented, as agreed to in the planning documents.

5. The software testing environment is documented and controlled.

(b) Data Required for the Software Verification Review. For the purpose of compliance findings for the software verification review, the software data shown in Table 3 should be made available to the FAA. The supporting software data should be under configuration control, as appropriate for the software level, prior to the review.

Software Data	**DO-178B Section**
Software Requirements Data	11.9
Design Description	11.10
Source Code	11.11
Software Verification Cases and Procedures	6.3.1-6.3.6, 11.13
Software Verification Results	11.14
Software Life Cycle Environment Configuration Index (test environment)	11.15
Software Configuration Index (test baseline)	11.16
Problem Reports	11.17
Software Configuration Management Records	11.18
Software Quality Assurance Records	11.19
Software Tool Qualification Data	12.2.3

Table 3. Data Availability for Software Verification Review

(c) Evaluation Criteria for Software Verification Review. The following DO-178B, Annex A, objectives apply to the software verification review and should be used as evaluation criteria: Tables A-1 (objective 3), A-5 (objective 7), A-6 (all objectives), A-7 (all objectives), A-8 (all objectives), A-9 (objectives 1-2), and A-10 (objective 3).

(4) Final Certification Software Review

(a) Identification of Final Certification Software Review. The final software build establishes the configuration of the software product considered by the applicant to comply with all the objectives of DO-178B. It is that version of the software intended to be used in the airborne application. The purpose of this review is to: determine compliance of the final software product with the objectives of DO-l78B, as defined by the software level and other software policy and guidance; ensure that all software development, verification, quality assurance, configuration management, and certification liaison activities are complete; ensure a software conformity review has been completed and the software complies; and review configuration indexes. The final certification software review should take place when the software project is completed and includes the following criteria:

1. Software conformity review has been performed and any deficiencies resolved.

2. Software Accomplishment Summary and Configuration Indexes have been completed and reviewed.

3. All software life cycle data has been completed, approved, and placed under configuration control.

(b) Data Required for Final Certification Software Review. For the purpose of this review, all software life cycle data of DO-178B should be available to FAA and/or DER. However, only the data shown in Table 4 is of special interest for this review. The supporting software data should be under configuration control, appropriate for the software level, prior to the review.

Software Data	**DO-178B Section**
Software Verification Results	11.14
Software Life Cycle Environment Configuration Index	11.15
Software Configuration index	11.16
Problem Reports	11.17
Software Quality Assurance Records (Software Conformity Review Report)	11.18
Software Accomplishment Summary	11.20

Table 4. Data Availability for Final Certification Software Review

(c) Evaluation Criteria for Final Certification Software Review. Evaluation criteria for this review includes all objectives of DO-178B, Annex A. Additionally, all software-related problem reports, action items, certification issues, etc. must be addressed prior to certification or authorization.

8. ADDITIONAL CONSIDERATIONS FOR THE SOFTWARE REVIEW PROCESS.

a. Although this notice proposes four types of review for FAA on-site reviews, the type, number, and extent of those reviews may not be suitable for every certification project and applicant. Additional considerations and alternative approaches may be appropriate. The following list of considerations may influence the level of the FAA involvement in the software review process:

(1) The software level(s), as determined by a system safety assessment.

(2) The product attributes (e.g. size, complexity, system functionality, software design).

(3) The use of new technologies or unusual design features.

(4) Proposals for novel software methods or life cycle model(s).

(5) The knowledge and previous success of the applicant in software development to comply with the objectives of DO-178B.

(6) The availability, experience, and authorization of software designees.

(7) The existence of issues associated with Section 12 of DO-178B in the project.

(8) The issuance of issue papers for software-specific aspects of the certification project.

b. On-site software reviews may be increased or decreased in number. Four reviews is a typical number for a Level A or Level B project; especially if no software DER is involved. Fewer or no reviews may be appropriate for some equipment manufacturers. Furthermore, reviews may be merged into a combined event or delegated to an authorized DER. It is the responsibility of the ACO engineer to determine the desired level of investigation, to plan the reviews, and to coordinate with the applicant. Criteria is being developed by the FAA to determine the appropriate level of FAA involvement in software projects. This criteria will be included in future policy.

9. PREPARING, CONDUCTING, AND DOCUMENTING THE SOFTWARE REVIEW. This section provides guidelines for preparing for the on-site review, conducting the on-site review, and recording and communicating the review results:

a. Prepare for the On-Site Review. The responsible certification engineer should assemble the review team. The team should include at least one person knowledgeable in software engineering, one person familiar with the type of system being evaluated, and a manufacturing inspector knowledgeable in software quality assurance and configuration management (if available). The certification engineer should coordinate with the applicant regarding the upcoming software review at least six weeks in advance and propose an agenda. To optimize the efficiency of the review team while on-site, the certification authority should request the applicant to send each team member the software plans identified in DO-178B, section 4.3, several weeks prior to the review. Each team member should review the plans prior to arriving at the applicant's facility. The certification engineer should prepare a short entry briefing to introduce the team members, restate the purpose of the review, and review the agenda. The applicant should provide a short briefing to facilitate an understanding of the system under review, the software life-cycle model, processes, tools used, and any additional considerations.

Note: The specific roles and responsibilities of the FAA software review team are being documented in future FAA policy.

b. Notify the Applicant. The ACO engineer should notify the applicant in writing regarding the FAA's expectations in the software review. The following information should be included in the notification letter:

(1) The purpose of the review and the type of review (i.e., planning, development, verification, or final).

(2) The date and duration of the review.

(3) A list of review participants (FAA personnel and designees) with contact information.

(4) A request that the software plans identified in DO-178B, section 4.3, be sent to each review participant.

(5) A request that pertinent life cycle data be made available at time of review.

(6) An indication of which DO-178B objectives will be assessed.

(7) A suggestion that the applicant conduct their own self-assessment prior to the review.

(8) A request that the responsible managers, developers, verification, configuration management, and quality assurance personnel be available for questions.

c. Conduct the On-site Review. A typical on-site review includes the following elements:

(1) Certification Authority Entry Briefing to Include: introduction of review team members; restatement of purpose of the review; and overview of the review agenda.

(2) Software Developer's Briefing to Include: availability of facilities; availability of life cycle data; personnel schedule constraints; overview of the system; interaction of the system with other systems; system architecture; software architecture; software life cycle model (including tools and methods); progress against previous action items or issue papers (if appropriate); current status of the development; and any additional considerations (per DO-178B, section 12).

(3) Certification Authority's Review of the Applicant/Developer's Process.

(4) Certification Authority's Review of Product.

d. Record the Review Results. The review results should be recorded; the record should include the following, as a minimum:

(1) A list of the each life cycle data item reviewed to include: document name; control identity; version and date; requirement identification (where applicable); source code module (where applicable); paragraph number (where applicable); and review results.

(2) The approach taken to establish the finding or observation.

(3) An explanation of the findings or observations as related to the objectives of DO-178B (documented with detailed notes). Each unsatisfied objective requires a summary of what was done and a discussion as to why the objective was not satisfied. Examples should be included, when necessary. This will ensure that the approach and findings can be understood and reconstructed at some future date.

(4) Any necessary actions for either the applicant or the FAA.

(5) Listing of all current or potential issue papers.

e. Deliver an Exit Briefing. The final briefing to the manufacturer under review should be factual and positive and should summarize the findings. Findings should be presented with specific reference to DO-178B, certification basis, policy, guidance, or other certification documentation. The manufacturer should be given the opportunity to respond to the findings.

f. Identify and Prepare Issue Papers (as needed). Issue papers are a means of documenting technical and certification issues that must be resolved prior to system certification. They provide the necessary communication between applicant and certification engineer and management. Issue papers should be identified, prepared, and resolved as soon as possible after the issue is discovered. Issue papers prepared for software-specific issues should be coordinated with FAA Headquarters (AIR-130) and the appropriate Directorate.

10. CONCLUSION. The information and procedures described in this notice promote clarification and consistent application of the software review process which is part of the Certification Liaison Process described in DO-178B. This notice does not replace or supersede AC 20-115B or DO-178B.

<< Original Signed by James C. Jones >>

James C. Jones
Manager, Aircraft Engineering Division,
Aircraft Certification Service